none none none



PN - JP2002055955 A20020220
PD - 2002-02-20
PR - JP20000238517 20000807
OPD - 2000-08-07
TI - METHOD AND SYSTEM FOR PERSONAL AUTHENTICATION
IN - NODA HIROTO; KAWASHIMA OSAMU;KAZUNO AKIRA
PA - DOCOMO SYSTEMS INC
IC - G06F15/00 ; H04Q7/38 ; H04L9/32 ; H04M3/42



TI - User authentication method for online shopping, involves acquiring calling party telephone number and password from access origin and compares it with registered information, for user authentication
PR - JP20000238517 20000807
PN - JP2002055955 A20020220 DW200239 G06F15/00 005pp
PA - (INSE-N) INS ENG KK
IC - G06F15/00 ;H04L9/32 ;H04M3/42 ;H04Q7/38
AB - JP2002055955 NOVELTY - The user ID and the calling party telephone number are stored beforehand. When the user accesses the terminal ( 1), the calling party telephone number from the access origin is acquired and compared with the registered number. When both confirm, the password is acquired from the access origin and verified. The user is authenticated based on the verification.
- DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for user authentication system.
- USE - User authentication for providing service such as online shopping.
- ADVANTAGE - Eliminates the illegal access by the third person as much as possible, hence ensures reliable security property.
- DESCRIPTION OF DRAWING(S) - The figure shows the components of user authentication system. (Drawing includes non-English language text).
- User terminal 1
- (Dwg.1/2)
OPD - 2000-08-07
AN - 2002-356719 [39]



PN - JP2002055955 A20020220
PD - 2002-02-20
AP - JP20000238517 20000807
IN - KAWASHIMA OSAMU;NODA HIROTO;KAZUNO AKIRA

PA - DOCOMO SYSTEMS INC

TI - METHOD AND SYSTEM FOR PERSONAL AUTHENTICATION

AB - PROBLEM TO BE SOLVED: To provide a method and a system for personal authentication with superior security, which can eliminate unauthorized access by a 3rd party as much as possible.

- SOLUTION: A user ID, a password, a telephone number for authentication, and a caller telephone number are used as elements for authenticating a registered person. The user ID and caller telephone number are previously registered and the password and telephone number for authentication are issued by a server 3 when the server is accessed.

I - G06F15/00 ;H04Q7/38 ;H04L9/32 ;H04M3/42

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－55955
（P2002－55955A）
(43)公開日　平成14年２月20日(2002.2.20)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　15/00 | ３３０ | Ｇ０６Ｆ　15/00 | ３３０Ｂ | ５Ｂ０８５ |
| | | | ３３０Ｃ | ５Ｊ１０４ |
| Ｈ０４Ｑ　7/38 | | Ｈ０４Ｍ　3/42 | Ｅ | ５Ｋ０２４ |
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｂ　7/26 | １０９Ｒ | ５Ｋ０６７ |
| Ｈ０４Ｍ　3/42 | | Ｈ０４Ｌ　9/00 | ６７３Ａ | |

審査請求　有　請求項の数３　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願2000－238517(P2000－238517)

(22)出願日　平成12年８月７日(2000.8.7)

(71)出願人　591144475
ドコモ・システムズ株式会社
東京都品川区西五反田四丁目31番18号

(72)発明者　川島　攻
東京都品川区西五反田四丁目31番18号　アイ・エヌ・エス・エンジニアリング株式会社内

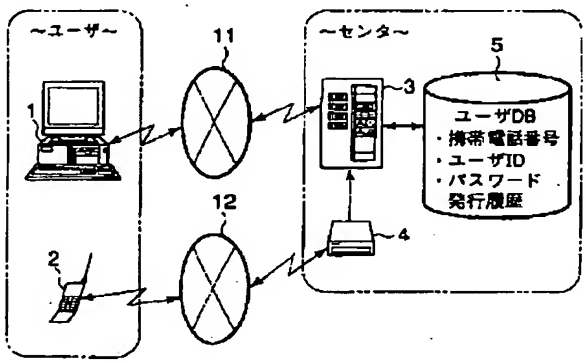
(72)発明者　野田　浩人
東京都品川区西五反田四丁目31番18号　アイ・エヌ・エス・エンジニアリング株式会社内

(74)代理人　100058479
弁理士　鈴江　武彦　（外５名）

最終頁に続く

(54)【発明の名称】　本人認証方法および本人認証システム

(57)【要約】
【課題】　第三者による不正なアクセスを極力排除することができるセキュリティ性にすぐれた本人認証方法および本人認証システムを提供できる。
【解決手段】　登録者本人を認証する要素として、ユーザＩＤ、パスワード、認証用電話番号、発信者電話番号を使用する。ユーザＩＤおよび発信者電話番号は予め登録され、パスワードおよび認証用電話番号はアクセス時にサーバ３から発行される。



【特許請求の範囲】
【請求項１】　端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合するステップと、
この照合結果が一致の場合に、任意のパスワードを特定の認証用電話番号と共にアクセス元の端末に送信するステップと、
前記認証用電話番号に基づく電話回線接続を受けた場合にその電話の発信者番号を識別するステップと、
この識別された発信者番号と予め登録されている発信者番号とを照合するステップと、
この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求するステップと、
この要求後、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと前記送信済みのパスワードとを照合するステップと、
この照合結果が一致の場合に、前記端末からのアクセス者が登録者本人であることを認証するステップと、
を備えたことを特徴とする本人認証方法。
【請求項２】　情報入力用の端末と、
所定のネットワークアドレスが設定され、前記端末からのネットワークを介したアクセスおよび外部からの電話回線による接続が可能な処理装置と、
この処理装置に設けられ、前記端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合し、この照合結果が一致の場合に、任意のパスワードを前記電話回線による接続のための認証用電話番号と共にアクセス元の端末に送信する第１制御手段と、
前記認証用電話番号に基づいて前記処理装置への電話回線接続があった場合にその電話の発信者番号を識別する識別手段と、
前記処理装置に設けられ、前記識別手段の識別結果と予め登録されている発信者番号とを照合し、この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求する第２制御手段と、
前記処理装置に設けられ、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと前記送信済みのパスワードとを照合し、この照合結果が一致の場合に、前記端末からのアクセス者が登録者本人であることを認証する第３制御手段と、
を具備したことを特徴とする本人認証システム。
【請求項３】　請求項２に記載の本人認証システムにおいて、
前記電話回線は、携帯電話器による通信が可能な無線電話回線であることを特徴とする本人認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、ネットワークを介したサービス提供などに用いられる本人認証方法および本人認証システムに関する。
【０００２】
【従来の技術】ネットワークを介したサービス提供たとえばオンラインショッピングでは、端末としてパーソナルコンピュータが使用され、サービスを提供する側の処理装置としてサーバコンピュータ（以下、サーバと略称する）が使用される。
【０００３】サーバにはユーザ（利用者）の識別情報いわゆるユーザＩＤが予め登録され、パーソナルコンピュータからのアクセスに際し、ユーザは自身のユーザＩＤを入力することになる。この入力されるユーザＩＤと登録済みのユーザＩＤとが照合され、両者が一致する場合のみ、サーバでのサービス提供が許可される。
【０００４】
【発明が解決しようとする課題】ユーザに与えられるユーザＩＤは、第三者に漏れることがある。ユーザＩＤが第三者に知られると、第三者がサーバにアクセスしてサービスを受けることが可能となり、まったく覚えのない商品の代金が正規のユーザに請求されるなど、正規のユーザに被害が及ぶことがある。これは、ユーザだけでなく、サービスを提供する側の業者にとっても、大きな問題となっている。
【０００５】この発明は上記の事情を考慮したもので、その目的とするところは、第三者による不正なアクセスを極力排除することができるセキュリティ性にすぐれた本人認証方法および本人認証システムを提供することにある。
【０００６】
【課題を解決するための手段】請求項１に係る発明の本人認証方法は、端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合するステップと、この照合結果が一致の場合に、任意のパスワードを特定の認証用電話番号と共にアクセス元の端末に送信するステップと、上記認証用電話番号に基づく電話回線接続を受けた場合にその電話の発信者番号を識別するステップと、この識別された発信者番号と予め登録されている発信者番号とを照合するステップと、この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求するステップと、この要求後、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと上記送信済みのパスワードとを照合するステップと、この照合結果が一致の場合に、上記端末からのアクセス者が登録者本人であることを認証するステップと、を備えている。
【０００７】請求項２に係る発明の本人認証システムは、情報入力用の端末と、所定のネットワークアドレスが設定され、上記端末からのネットワークを介したアクセスおよび外部からの電話回線による接続が可能な処理

装置と、この処理装置に設けられ、上記端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合し、この照合結果が一致の場合に、任意のパスワードを上記電話回線による接続のための認証用電話番号と共にアクセス元の端末に送信する第１制御手段と、上記認証用電話番号に基づいて上記処理装置への電話回線接続があった場合にその電話の発信者番号を識別する識別手段と、上記処理装置に設けられ、上記識別手段の識別結果と予め登録されている発信者番号とを照合し、この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求する第２制御手段と、上記処理装置に設けられ、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと上記送信済みのパスワードとを照合し、この照合結果が一致の場合に、上記端末からのアクセス者が登録者本人であることを認証する第３制御手段と、を備えている。

【０００８】請求項３に係る発明の本人認証システムは、請求項２に係る発明において、電話回線について限定している。電話回線は、携帯電話器用の無線電話回線である。

【０００９】

【発明の実施の形態】以下、この発明の一実施形態について図面を参照して説明する。

【００１０】図１に示すように、情報入力用の端末として、ユーザ宅にパーソナルコンピュータ１が設置されている。２は携帯電話器で、ユーザが専用に所持している。

【００１１】一方、処理装置として、管理センタにサーバコンピュータ（以下、サーバと略称する）３が設置されている。サーバ３には所定のネットワークアドレスが設定されており、このネットワークアドレスに基づき、上記パーソナルコンピュータ１からサーバ３へのネットワーク１１を介したアクセスが可能となっている。

【００１２】また、サーバ３は、特定の認証用電話番号に基づいて、外部からの電話回線接続を受付ける機能を備えている。すなわち、上記携帯電話器２から特定の認証用電話番号を入力することにより、その携帯電話器２とサーバ３とが無線電話回線（デジタル電話回線、携帯電話網とも称す）１２を介して相互接続される。

【００１３】さらに、サーバ３に対し、発信者番号受信装置（識別手段）４およびユーザデータベース（以下、ユーザＤＢと略称する）５が接続されている。

【００１４】発信者番号受信装置４は、サーバ３への電話回線接続があった場合に、その電話から発せられるデータを受信し、そのデータに基づいて同電話の発信者番号（例えば携帯電話番号）を識別する。

【００１５】ユーザＤＢ５には、登録を許可された者だけに与えられる識別情報いわゆるユーザＩＤ（加入者ＩＤとも称す）が登録されるとともに、その登録者が所持している携帯電話番号（または自宅電話番号）が発信者電話番号としてユーザＩＤに対応付ける形で登録され、さらに、後述のパスワード発行履歴が逐次に追加記憶される。

【００１６】そして、サーバ３は、たとえばネットワークショッピングのサービスを提供するためのホームページ画像情報を内部メモリに有するとともに、主要な機能として次の［１］～［４］を有している。

【００１７】［１］パーソナルコンピュータ１からのアクセスに際し、同パーソナルコンピュータ１で入力されるユーザＩＤとユーザＤＢ５に登録されているユーザＩＤとを照合し、この照合結果が一致の場合に、任意のパスワードをランダムに選定し、そのパスワードをユーザＩＤに対応付けた形のパスワード発行履歴としてユーザＤＢ５に記憶するとともに、同パスワードを電話回線接続用の特定の認証用電話番号と共にアクセス元のパーソナルコンピュータ１に送信する第１制御手段。

【００１８】［２］発信者番号受信装置４で識別された発信者番号とユーザＤＢ５に登録されている発信者番号とを照合し、この照合結果が一致の場合に、アクセス元のパーソナルコンピュータ１または電話回線接続の発信元に対しパスワードの入力を要求する第２制御手段。

【００１９】［３］アクセス元のパーソナルコンピュータ１または電話回線接続の発信元から入力されるパスワードと上記送信済みのパスワード（ユーザＤＢ５内のパスワード発行履歴）とを照合し、この照合結果が一致の場合に、パーソナルコンピュータ１からのアクセス者が登録者本人であることを認証する第３制御手段。

【００２０】［４］アクセス者が登録者本人であることを認証したとき、パーソナルコンピュータ１からのアクセスに応じたネットワークショッピングのサービスの提供を許可する第４制御手段。

【００２１】つぎに、上記の構成の作用を図２を参照しながら説明する。ネットワークショッピングのサービスを受けようとするユーザが自宅のパーソナルコンピュータ１でサーバ３のネットワークアドレスを入力すると、パーソナルコンピュータ１がネットワーク１１を介してサーバ３に接続される。この状態で、ユーザがパーソナルコンピュータ１からユーザＩＤを入力すると、そのユーザＩＤとユーザＤＢ５に登録されているユーザＩＤとが照合される。

【００２２】ユーザＩＤの照合が不一致の場合、アクセス者が登録ユーザではないとの判断の下に、アクセス拒否通知（文字データ）がサーバ３からパーソナルコンピュータ１に送られる。

【００２３】ユーザＩＤの照合が一致の場合、サーバ３において任意のパスワードがランダムに選定され、そのパスワードがパスワード発行履歴の形でユーザＤＢ５に記憶されるとともに、同パスワードが認証用電話番号と共にアクセス元のパーソナルコンピュータ１に送信され

る。送信されたパスワードおよび認証用電話番号は、パーソナルコンピュータ１のディスプレイで表示される。

【００２４】ユーザは、ディスプレイを見てパスワードおよび認証用電話番号を確認し、そのうちの認証用電話番号を自身の携帯電話器２で入力する。すると、携帯電話器２とサーバ３とが無線電話回線１２を介して接続され、その接続に伴い、携帯電話器２の発信者番号（携帯電話番号）が発信者番号受信装置４で識別される。そして、識別された発信者番号とユーザＤＢ５に登録されている発信者番号とが照合される。

【００２５】発信者番号の照合が不一致の場合、アクセス者が登録ユーザではないとの判断の下に、アクセス拒否通知（音声データ）がサーバ３から携帯電話器２に送られる。

【００２６】発信者番号の照合が一致の場合、電話回線接続の発信元である携帯電話器２（またはアクセス元のパーソナルコンピュータ１）に対しパスワードの入力が要求される。

【００２７】ユーザは、入力要求に応じて、すでに確認しているパスワードを携帯電話器２から入力する。このとき、入力に使用された携帯電話器２の発信者番号が発信者番号受信装置４で識別され、その識別された発信者番号に対応するユーザＩＤがユーザＤＢ５において割り出され、かつ割り出されたユーザＩＤに基づいてユーザＤＢ５内のパスワード発行履歴から送信済みのパスワードが検索される。そして、検索されたパスワードと上記入力されたパスワードとが照合される。

【００２８】パスワードの照合が不一致の場合、アクセス者が登録ユーザではないとの判断の下に、アクセス拒否通知（音声データ）がサーバ３から携帯電話器２に送られる。

【００２９】なお、パスワードの入力受付は一定時間内に制限される。入力要求が出されてから一定時間内にパスワードが入力されなかった場合、パスワード照合が不一致の場合と同様に、アクセス拒否通知（音声データ）がサーバ３から携帯電話器２に送られる。

【００３０】パスワードの照合が一致の場合は、パーソナルコンピュータ１からのアクセス者が登録者本人であるとの認証がなされ、サーバ３においてサービスの提供が許可される。同時に、許可の旨の通知（音声データ）がサーバ３から携帯電話器２に送られる。

【００３１】ユーザは、許可通知に従い、パーソナルコンピュータ１を介してホームページ画像を閲覧し、ネットワークショッピングのサービスを受けることができる。

【００３２】以上のように、登録者本人を認証する要素として、ユーザＩＤ、パスワード、認証用電話番号、発信者電話番号を使用することにより、従来のようにユーザＩＤのみを認証に使用する場合に比べ、セキュリティ効果が大幅に向上する。

【００３３】たとえば、ユーザＩＤが第三者に知られても、その第三者が番号登録済みの携帯電話器２または自宅電話器を持たない限り、サーバ３でのサービスを受けることは不可能であり、第三者による不正なアクセスを極力排除することができる。サービスを提供する側にとっては高い信頼性を確保することができる。

【００３４】なお、ユーザＩＤの具体例として、携帯電話器２や自宅電話器の電話番号を使用してもよい。また、上記実施形態では、ネットワーク接続用の端末としてパーソナルコンピュータ１を用い、電話回線接続手段として携帯電話器２を用いたが、そのパーソナルコンピュータ１および携帯電話器２に代えて、ネットワーク接続の機能および電話回線接続の機能を併せ持つ複合型携帯電話器を使用してもよい。その他、この発明は上記実施形態に限定されるものではなく、要旨を変えない範囲で種々変形実施可能である。

【００３５】

【発明の効果】以上述べたようにこの発明によれば、登録者本人を認証する要素として、ユーザＩＤ、パスワード、認証用電話番号、発信者電話番号を使用するようにしたので、第三者による不正なアクセスを極力排除することができるセキュリティ性にすぐれた本人認証方法および本人認証システムを提供できる。

【図面の簡単な説明】

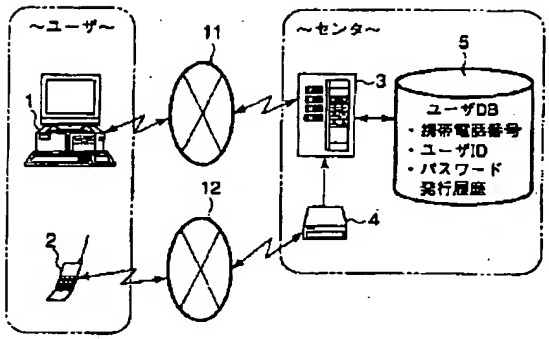
【図１】一実施形態の構成を示すブロック図。

【図２】同実施形態の作用を説明するための図。

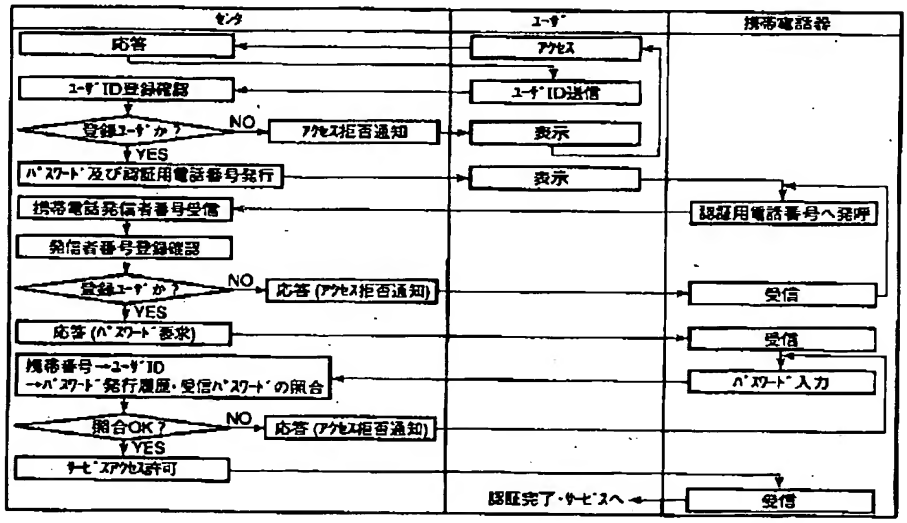
【符号の説明】

1…パーソナルコンピュータ（端末）、2…携帯電話器、3…サーバコンピュータ（処理装置）、4…発信者番号受信装置、5…ユーザデータベース

【図1】




【図2】




---

フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | FI | テーマコード(参考) |
|---|---|---|---|
| | | H04L 9/00 | 673B |

(72)発明者 数野 顕
東京都品川区西五反田四丁目31番18号 アイ・エヌ・エス・エンジニアリング株式会社内

Fターム(参考) 5B085 AE03 AE23
5J104 AA07 KA01 KA07 NA05 PA02
5K024 AA62 CC09 CC11 DD01 GG05
5K067 AA32 BB04 DD15 DD17 EE02
EE10 EE16 GG01 HH22